

Claims

- [c1] A method for autonomic administration isolation for a secure remote management in a computer network, the method comprising the steps of:
- (a) isolating administrative access to a plurality of client systems in a computer network via a data center; and
 - (b) utilizing the data center to control remote initiation of services in the plurality of client systems by an administrative system.
- [c2] The method of claim 1 wherein the utilizing step (b) further comprises the step of (b1) verifying authentication of the administrative system by the data center.
- [c3] The method of claim 2 further comprising the step of (b2) receiving service commands from the authenticated administrative system in the data center.
- [c4] The method of claim 3 further comprising the step of (b3) determining in the data center whether the authenticated administrative system has authorization to perform the service commands in the managed client systems.
- [c5] The method of claim 4 further comprising the step of (b4) issuing trusted messages from the data center to the managed client systems when the authenticated administrative system does have authorization to perform the service commands.
- [c6] The method of claim 5 further comprising (c) validating and decrypting the trusted messages in the managed client systems to perform the service commands.
- [c7] An autonomic system for selective administration isolation for secure remote management in a computer network, the system comprising:
- a network;
 - at least one administrator system coupled to the network;
 - at least one client system coupled to the network; and
 - a data center coupled to the at least one administrator system and to the at least one client system via the network, the data center for isolating administrative access to the at least one client system and controlling remote initiation of services in the at least one client system by the at least one

administrative system.

- [c8] The system of claim 7 wherein the at least one administrator system includes authentication capabilities via an embedded security chip for unique system identification and biometric identification for unique user identification.
- [c9] The system of claim 7 wherein the data center verifies authentication of the at least one administrative system.
- [c10] The system of claim 9 wherein the authenticated at least one administrative system sends service commands to the data center.
- [c11] The system of claim 10 wherein the data center determines whether the authenticated administrative system has authorization to perform the service commands in the at least one client system.
- [c12] The system of claim 11 wherein the data center issues trusted messages to the at least one client system when the authenticated administrative system does have authorization to perform the service commands.
- [c13] The system of claim 12 wherein the at least one client system validates and decrypts the trusted messages to perform the service commands.
- [c14] The system of claim 9 wherein the network further comprises a world wide web network.
- [c15] A computer readable medium containing program instructions for autonomic administration isolation in a computer network for a secure remote management, the program instructions for:
- (a) isolating administrative access to a plurality of client systems in a computer network via a data center; and
 - (b) controlling remote initiation of services in the plurality of client systems by an administrative system via the data center.
- [c16] The computer readable medium of claim 15 further comprising (b1) verifying authentication of the administrative system by the data center.
- [c17] The computer readable medium of claim 16 further comprising (b2) receiving

service commands from the authenticated administrative system in the data center.

[c18] The computer readable medium of claim 17 further comprising (b3) determining in the data center whether the authenticated administrative system has authorization to perform the service commands in the managed client systems.

[c19] The computer readable medium of claim 18 further comprising (b4) issuing trusted messages from the data center to the managed client systems when the authenticated administrative system does have authorization to perform the service commands.

[c20] The computer readable medium of claim 19 further comprising (c) validating and decrypting the trusted messages in the managed client systems to perform the service commands.